Diese Website verwendet Cookies von Google, um Dienste anzubieten und den Traffic zu analysieren. Deine IP-Adresse und dein User-Agent werden zusammen mit Messwerten zur Leistung und Sicherheit für Google freigegeben. So können Nutzungsstatistiken generiert, Missbrauchsfälle erkannt und behoben und die Qualität des Dienstes gewährleistet werden.

WEITERE INFORMATIONEN OK

An unending variety of topics

Friday, September 28, 2007

Secure time broadcast

From my article Advances in Distributed Security:

> Broadcasts using sound or radiation, from sources such as bell towers, radio towers, satellites, and pulsars, must send out the same value to every receiver. A remote beacon such as a pulsar has perfect security: the access structure is any party, and its complement, the attack structure, is the empty set. For human controlled broadcasts, the attack structure consists only of the broadcaster and the access structure is any receiver.
>
> Natural broadcasts are thus immune to the problem, described in the discussion of the Byzantine Generals problem below, of a transmitter sending different values to different receivers. Indeed, as we will see below, distributed researchers have gone to great lengths just to recreate this simple property on the Internet with logical broadcast protocols.
>
> Nature provides clocks that are oblivious to the malicious intentions of any outside parties. In the case of a remote high-energy system such as a pulsar, this means anybody. Pulsars are many orders of magnitude more accurate than random delays that face attackers on the Internet. If critical Internet servers were synchronized to natural clocks in a secure and timely fashion, they would be immune to attacks that relied on uncertainties in timing.

More here.

Detecting pulsars is still, alas, a difficult process, but not so hard that amateurs have had no success doing so. Amateurs have had some success tracking pulsars with software defined radio and quagi antennas combined with digital signal processing.

Posted by Nick Szabo at 12:01 PM

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

Blog Archive

- ► 2018 (1)
- ► 2017 (3)
- ► 2016 (4)
- ► 2015 (3)
- ► 2014 (3)
- ► 2013 (3)
- ► 2012 (8)
- ► 2011 (12)
- ► 2010 (9)
- ► 2009 (29)
- ► 2008 (55)
- ▼ 2007 (47)
  - ► December (1)
  - ► October (2)
  - ▼ September (8)
    - Secure time broadcast
    - Real options analysis for space projects
    - Tamper evident numbers
    - Mining the vasty deep (iii)
    - Partial and total orders
    - Institutional changes prerequisite to the industri...
    - Secure property titles
    - Bilinear group cryptography
  - ► August (10)
  - ► July (4)
  - ► June (4)
  - ► May (8)
  - ► April (1)
  - ► March (2)
  - ► February (4)
  - ► January (3)
- ► 2006 (130)
- ► 2005 (44)

Simple theme. Powered by Blogger.